Győrű Attila
Nemzetközi Jogi Tanszék
Témavezető: Kardos Gábor egyetemi tanár

Privacy és terrorizmus

I. rész[1]

1. Bevezetés

Jelen cikk felvezetését is lehetne azzal a gyakran használt fordulattal kezdeni, hogy a címben szereplő téma nem új, az már évszázadok vagy akár évezredek óta jelen van az emberiség történetében. Tény, hogy a *privacy*, – mely fogalom bemutatása a következő fejezet célja – mint az átfogó értelemben vett magánszféra és annak védelme, nem új keletű, hanem már hosszú ideje részét képezi történelmünknek. A terrorizmus szempontjából nézve még inkább egyértelmű, hogy a jelenség „ősidők" óta jelen van világunkban.[2]

Az elmúlt néhány évtizedben azonban a két fogalom összefüggései egészen más értelmet nyertek, és a kérdés jelentősége ma már elvitathatatlan. A döntő fontosságú esemény a 2001. szeptember 11-i Egyesült Államok elleni terrortámadás, amely után a terrorizmus és a terrorizmus elleni küzdelem, részben az USA által meghirdetett „*War on Terror*" hadjárat eredményeként a világ figyelmének fókuszába került. A jelenség aktualitását csak növeli az elmúlt években a migráció nagyságrendi változása és az Iszlám Állam felemelkedése. A kérdés sajnos olyannyira aktuális, hogy jelen sorok írásakor is újabb terrortámadástól hangos a nemzetközi sajtó, 2017. március 22-én Londonban egy merénylő 5 embert ölt meg a Westminster előtt elkövetetett merényletben. Az arra adott brit válasz számos eleme közül az egyik pedig már össze is kapcsolja a címben említett két fogalmat, Amber Rudd brit belügyminiszter felszólította a közösségi média (Facebook, Twitter, WhatsApp, Google, Apple) képviselőit, hogy működjenek közre a terroristák világhálón megvalósított kommunikációjának és a világhálón megjelenő terrorista propaganda kiszűrésében és törlésében.[3] Mondani sem kell, hogy a kérdés masszívan felvet *privacy* aspektusokat is. Sajnálatos módon az eset olyannyira nem

[1] A tanulmány II. részét a Themis 2017. dcemberi számában közöljük.

[2] A terrorizmus már az ókorban megjelent, despotikus uralkodók gyakran terrorizáltak leigázott népeket. A terror eszközét alkalmazták az asszírok a leigázott népek ellen, vagy Spártában a harcias dór törzsek terrorizáltak őslakos helótákat. Szintén jó példa a terrorizmusra a rómaiaknak a gladiátorok és a rabszolgák ellen alkalmazott módszerei.

[3] http://www.voanews.com/a/britain-social-media-sites-cleared-jihadist-postings/3783658.html

egyedülálló, hogy néhány nappal később 2017. április 3-án Szent Péterváron az egyik metrószerelvényen robbant fel pokolgép, mely 14 áldozattal járt.[4] 2017. április 7-én pénteken Stockholmban egy teherautó hajtott a gyalogosok közé egy sétálóutcában, a következmény 4 áldozat.[5] Jelen ügyekben folyik a nyomozás, de a stockholmi esetnél az elkövető már most elismerte, hogy terrortámadást valósított meg. Csak ezeket a példákat említve, a napi események alapján is jól látszik a cikk témájának kiemelt jelentősége.

Már a bevezetőben fel kell hívni a figyelmet egy fontos jelenségre, ami lényeges indoka annak, hogy ez a téma ekkora társadalmi jelentőséggel rendelkezik. Amikor a *privacy* és terrorizmus összefüggéseiről beszélünk, akkor nem kizárólag arról van szó, hogy terrorcselekményt elkövetett személyek személyes adatai egy nyomozás során milyen védelmet élveznek. Ez a terület, tehát a gyanúsítottak *privacyhez* fűződő jogának korlátozása társadalmilag jobban elfogadott és jogilag alaposabban szabályozott. A kérdés sokkal inkább az, hogy egy potenciális terrortámadás megelőzése érdekében folytatott általános, mondhatni konkrét cél nélküli információgyűjtés, adatbányászat mennyiben indokolható egy demokratikus társadalomban. Az üzenet viszonylag egyszerű, mindenkit úgy kell vizsgálni, mint egy potenciális terroristát annak érdekében, hogy kiszűrjük közülük a valós terroristákat. Egyszerű, de felettébb vitatható üzenet egy jogállamban.

Kétrészes cikkem első részében bemutatom a két fogalom meghatározásának nehézségeit. Ezt követően a privacy védelmének és korlátozásának modelljeit tárgyalom a terrorizmus elleni fellépésben, részletesen elemezve az Európai Unió gyakorlatát. Cikkem második részében bemutatom az USA gyakorlatát, majd ismertetem azokat az aspektusokat, melyek előre vetíthetik a két szembenálló rendszer közötti konfliktus bizonyos fokú feloldásának lehetőségét.

2. Fogalmi meghatározások

A cikk témáját adó mindkét fogalomról elmondható, hogy komplexitásuk miatt azok meghatározása jelentős nehézségekbe ütközik, sőt már önmagában a definíció szükségessége is vita tárgya. Jelen fejezetben e fogalmak meghatározásához kísérlek meg tudományos és gyakorlati szempontokat adni.

[4] http://www.telegraph.co.uk/news/2017/04/03/saintpetersburg-bombing-casualties-explosion-metro-train/
[5] http://edition.cnn.com/2017/04/11/europe/stockholm-terror-attack-rakhmat-akilov/ https://www.nytimes.com/2017/04/11/world/europe/stockholm-terror-attack.html?_r=0

a) A privacy fogalma

A zavartalan magánélethez való jog bizonyos aspektusai egyidősek az emberiséggel[6], azonban általános elismerése és intézményes védelme csak a XIX. század második felében jelent meg az Egyesült Államokban.[7] Az európai országok, bár bizonyos fokú lemaradással kezdtek foglalkozni a témával, mára a védelem szintjét tekintve számos aspektusban megelőzték az USA által működtetett rendszert. Ennek elsődleges indoka, hogy a *privacy* mind az Európa Tanács, mind az Európai Unió alapjogvédelmi rendszerében fontos szerepet tölt be. Az privacy felértékelődésének remek példája az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), amely 2016. május 24-én lépett hatályba és 2018. május 25-től lesz alkalmazandó. Ez a jogszabály a *privacy* adatvédelmi elemeinek az egész Európai Unió területén egységes és a korábbinál erősebb védelmét biztosítja.

A privacy fogalmi meghatározásának központi eleme az emberi lét két szférája, nevezetesen a magánszféra és a külvilág közötti határ meghúzása. Ezen túlmenően azonban a témával foglalkozó szerzők a lehető legszélesebb skálán igyekeznek megmagyarázni vagy körülírni e fogalom jelentését. Néhány példát említve a nevesebb szerzők megközelítéseiből, Warren és Brandeis szerint a *privacyhez* való jog nem más, mint jog arra, hogy egyedül legyünk.[8] Alan Westin szerint a *privacy* egyének, egyének csoportjai és intézmények az iránti igénye, hogy meghatározhassák, a rájuk vonatkozó információk mikor, hogyan és milyen mértékben juthatnak mások tudomására.[9] Ez utóbbi definició abba a csoportba tartozik, amely hangsúlyozza a privacy információs oldalát.

Bizonyos definíciókban megjelenik a *privacy* fizikai oldala is, például Sissela Bok szerint a *privacy* a nem kívánt külső hozzáférés elleni

[6] Ahogy a privacy témájú tanulmányok közé sorolható egyik alapmű is írja, „az, hogy az ember személyének és tulajdonának teljes védelmet kell élveznie, egy alapelv, amely egyidős a common law rendszerével, de időről időre szükséges ismét definiálni ezen védelem természetét és mértékét.” (WARREN and BRANDEIS: The Rights to Privacy Harward Law review Vol. IV. December 15, 1890 No. 5)

[7] A téma egyik alapműve is ebben az időszakban született meg, lásd. 3. lábjegyzet.

[8] WARREN and BRANDEIS: uo.

[9] Alan WESTIN (1967): Privacy and Freedom. New York: Atheneum

védelmet jelenti, akár fizikai hozzáférésről, akár személyes adatok védelméről van szó.[10]

A modern kor szempontjait is figyelembe vevő megközelítés szerint a *privacy* kulcsfontosságú lencse, melyen keresztül sok új technológia, különösen a megfigyelési technológiák kritizálható.[11]

Számos meghatározást lehetne még idézni, amelyek többé-kevésbé kiemelik a *privacy* egy-egy aspektusát, azonban számomra sokkal teljesebb képet adnak azok a meghatározási kísérletek, amelyek e fogalmat nem definícióként, hanem főbb szempontjainak komplex rendszereként kívánják bemutatni. Ennek egyik jellemző példája egy magyar szerző Szabó Máté Dániel műve, akinek rövid definíciója szerint a *privacy* nem más, mint az egyén joga ahhoz, hogy magáról döntsön. Ő is megkülönbözteti a *privacy* fizikai és információs oldalát és e második elemet vizsgálva az alábbi következtetésre jut: *„Az információs önrendelkezési jog részben az egyénnek a rá vonatkozó ismeretek feletti rendelkezési joga. Ennek van pozitív és negatív oldala.*

Aa) Pozitív oldala, hogy ez a jog az önkifejezés joga. Az egyénnek ezek szerint joga van ahhoz, hogy megmutathassa a külvilágnak saját magát, illetve saját magának azt a részét, amit meg akar mutatni.

Ab) Negatív értelemben ennek a jognak a része az eltitkolás és a rejtőzködés joga. Az egyént tehát az önkifejezés jogának ellenkezője is megilleti: joga van ahhoz is, hogy eltitkoljon magából bármit, vagyis negatív értelemben gyakoroljon ellenőrzést a saját magára vonatkozó ismeretek felett.

Az információs önrendelkezés része az egyénnek az a joga is, hogy a külvilágra vonatkozó, de őt valamilyen módon érintő ismeretek felett ellenőrzést gyakoroljon.

Ba) Pozitív értelemben ez a jog a külvilág megismerésének szabadságát jelenti, vagyis azt, hogy az egyénnek joga van a tájékozottsághoz.

Bb) Az egyént azonban megilleti az előbb említett jog ellenkezője is, a külvilágtól való elzárkózás joga, a nemtudás joga, a robinsoni élethez való jog.”[12]

Ezt követően a szerző tisztázza a privacy és az adatvédelem viszonyát, bemutatva, hogy a két fogalom csak részben fedi egymást, és a privacy jóval tágabb kört foglal magában, mint csak az adatvédelmet.

[10] Sissela BOK (1983): Secrets. On the Ethics of Concealment and Revelation. New York: Pantheon Books
[11] David LYON: Surveillance after September 11 (Cambridge: Polity Press, 2003).
[12] SZABÓ Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. 2005. 47.

Színvonalas levezetésében arra a megállapításra jut, hogy az Ab) pont tartalmát, az eltitkolás jogát a személyes adatok védelme teljes egészében lefedi, a Bb) pontban tárgyalt tartalmi elemeket, az elzárkózás jogát csak részben szolgálják adatvédelmi szabályok. Az önkifejezésnek az Aa) pontban leírt jogát azonban az adatvédelem eszközrendszere egyáltalán nem garantálja. A személyes adatok védelméhez való jog ugyanígy nem biztosítja a külvilág megismerésének a Ba) pontban körülírt jogát sem.

A jelen tanulmány szempontjából a leghasznosabb megközelítést azok a szerzők képviselik, akik nem próbálják meg definiálni a privacy fogalmát, hanem bemutatják annak főbb elemeit és a főbb elemeket érintő intézkedések csoportjait. Ennek a megközelítésnek egyik képviselője Roger Clarke, aki 1997-ben készített tanulmányában a privacy 4 fajtáját különbözteti meg, melyek a következők: a személyhez fűződő privacy, a személyes adatokhoz fűződő privacy, a viselkedéshez fűződő privacy és a személyes kommunikációt érintő privacy (*privacy of the person, privacy of personal data, privacy of personal behavior, privacy of personal communication*).[13]

Értelmezése szerint a személyhez fűződő privacy, a testi integritáshoz fűződő jogokat jelenti. Nevezetesen, hogy az ember ne válhasson kínzás, kegyetlen, embertelen vagy megalázó bánásmód alanyává, erőszakkal, engedélye nélkül ne hajthassanak végre rajta orvosi beavatkozásokat (természetesen a sérült érdekében álló kivételes eseteket nem számítva), testnedveiből és testszöveteiből kényszerrel ne vehessenek mintákat, és biometrikus eszközöket csak korlátozásokkal alkalmazhassanak. Ez egyben a különféle megfigyelési technológiák korlátozását is jelenti.

A viselkedéshez fűződő privacy a különböző személyes szokások (vallási vagy szexuális szokások, politikai tevékenység stb.) megismerése és nyilvánosságra hozatala elleni védelmet biztosítja.

A személyes kommunikációt érintő privacy a telefon, e-mail és a virtuális kommunikáció más formáinak, valamint a személyes kommunikáció megfigyelése elleni védelmet jelenti.

A személyes adatokhoz fűződő privacy elsősorban az adatvédelmi kérdésekkel foglalkozik. Álláspontom szerint ide sorolhatók a tömeges adatgyűjtési technológiák is, melynek egyik jellemző példája az adatbányászat. Clarke szerint ez utóbbi kettő az 1980-as évek óta annyira

[13] Roger CLARK: Introduction to dataveillance and Information Privacy, and Definitions of Terms, Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html

összefonódott, hogy manapság nehezen határolhatók el egymástól, a kettőt együtt gyakran információs privacy néven használjuk.

Rachel L. Finn, David Wright és Michael Friedewald 2013-ban írt tanulmányukban ezt a kategorizálást fejlesztik tovább, és a privacy 7 fajtáját azonosítják, mivel véleményük szerint a modern kor technológiai fejlődésére adandó hatékony válaszhoz a Clarke-féle kategorizálás bővítése szükséges.[14] Tanulmányukban a viselkedéshez fűződő privacy fogalmát kettébontják a viselkedéshez és a cselekvéshez fűződő privacy-re. Személyes véleményem szerint ez a bontás nem ad különösebb hozzáadott értéket a privacy hatékonyabb védelméhez, mivel a viselkedés magában foglalja a különböző cselekvéseket is. A személyes adatokhoz fűződő privacy kiegészítése a képmás védelmével már érdekesebb kérdéseket vet fel. A szerzők a kiegészítést mindössze azzal indokolják, hogy ez is egyfajta személyes adat, melyre manapság kiemelt figyelmet kell fordítani. Teljesen egyetértve ezzel a véleménnyel, szeretném még erőteljesebben hangsúlyozni a kiegészítés jelentőségét, mivel a jogszabályi követelmények ellenére a mai napig nem egyértelmű a köztudatban, hogy a természetes személy képmása szintén személyes adatnak minősül akkor is, ha az információ birtokosa azt közvetlenül nem tudja egy névhez kapcsolni. Ez a kérdés különösen fontos a drónok (Unmanned Aircraft Systems, UASs) fedett alkalmazása estén, mellyel az érintettek gyakorlatilag észrevétlenül figyelhetők meg, sok esetben azonban olyan módon, hogy a megfigyelő nem is tudja, hogy ki a megfigyelt vagy kik a felvételeken szereplő személyek. Könnyű azonban belátni, hogy egy arcfelismerő szoftver alkalmazásával az érintettek könnyen azonosíthatók.

A szerzők három új csoportot is alkotnak, melyek részben a legmodernebb technológiákra is figyelemmel vannak, részben az említett csoportokból emelnek ki különleges jelentőségű elemeket.

Az 5. típus a gondolatokhoz és érzelmekhez fűződő privacy. Az emberek legszemélyesebb joga, hogy gondolataikat és érzelmeiket szabadon alakíthassák és azt másokkal ne osszák meg. A személyhez fűződő privacy úgy határolható el a gondolatokhoz és érzelmekhez fűződő privacy fogalmától, mint a test a lélektől: ezek külön-külön dimenziók, de elválaszthatatlanul össze is függnek egymással.

A 6. típus a tartózkodási hely meghatározásához fűződő privacy. Ennek lényege, hogy az embereknek joguk van ahhoz, hogy a saját magánterületükön, de még a nyilvános helyeken is azonosítás, követés és

[14] Rachel L. FINN, David WRIGHT and Michael FRIEDEWALD: Seven Types of Privacy 2013. Frauenhofer Institue for Systems and Innovation Research

monitorozás nélkül tartózkodhassanak, otthonukban emellett joguk van a magányhoz. Ez az egészséges és működő demokrácia szintén alapvető követelménye. Senkinek nem lehet kérdéses, hogy ide tartozik a közterületi kamararendszerek alkalmazása vagy ennek a privátszférába jobban beavatkozó változata, a kamerarendszer esetleg arcfelismerő szoftverekkel együtt alkalmazva. Legalább ennyire fontosak azonban ma még kevésbé ismert témák is, mint a földrajzi lokáció meghatározása a mobiltelefon GPS koordinátáinak követésével, az autóba épített GPS követése vagy például a városi tömegközlekedési bérlet- vagy taxirendelési szokások megfigyelése.

A 7. típus az egyesülési joghoz fűződő privacy vagy csoportos privacy, mely az emberek azon jogát érinti, hogy szabadon csatlakozhassanak pártokhoz, érdekvédelmi szervezetekhez vagy egyéb csoportosulásokhoz, melyek keretében egyénileg vagy másokkal együtt kinyilváníthatják véleményüket. Természetesen mindenkinek joga van ezek ellenkezőjére is, nevezetesen, hogy akaratuk ellenére ne sorolják őket semmilyen csoportba. Ennek a témának is vannak azonban kevésbé ismert, de legalább ilyen jelentős aspektusai, melyek érintik a csoporttól való megkülönböztetéshez való jogot is. Ilyen pl. a DNS elemzések kérdése, melyek alapján egyének például meghatározott rokonsághoz vagy etnikai csoporthoz sorolhatók.

A privacy értelmezését érintően elmondható, hogy a fogalom pontos meghatározását nyelvi korlátok is gátolják. Álláspontom szerint mindössze az angol nyelvű privacy kifejezés az, amely e fogalom jelentését viszonylagos pontossággal körül tudja írni. Más nyelvek azonban nem tartalmazzák ennek a szónak a szinonimáját, például a magyar magánélet szó is csak részben fejezi ki a privacy szó jelentését, ahogy ezt jelen fejezetben be is mutattam.

b) A terrorizmus fogalma

Az angol nyelvű irodalomban források sokasága áll rendelkezésre, melyek a terrorizmus fogalmának meghatározásával foglalkoznak. A magyar szakirodalomban kevesebb tanulmány született ilyen témában.

A kérdés összetettségét jól szemlélteti az alábbi okfejtés: „*A terrorizmus elleni hatékony fellépés egyik legalapvetőbb kérdése annak meghatározása, mely magatartások tartoznak ebbe a kategóriába. A terrorizmus fogalmának meghatározása több évtizedes célkitűzése a nemzetközi közösségnek, melynek eredményeként számos fogalom született mind a nemzetközi, mind a nemzeti jogban, azonban átfogó*

definíció sikeres megalkotásáról nemzetközi területen nem beszélhetünk. A nemzetközi politika és jog képviselőinek általános véleménye, hogy kevés szó létezik, mely ilyen mértékben pontatlan, szubjektív és politikai viták tárgya, mint a terrorizmus. Még az is vitatott kérdés, hogy a fogalom meghatározása milyen mértékben szükséges a terrorizmus elleni hatékony fellépéshez. Olyan elem-e, mely valóban nélkülözhetetlen, vagy csak egy a számos elem közül, mely hatékonyabbá teheti a terrorizmusra adható nemzetközi válaszokat, azonban a rendszer a jelenlegi politikai és jogi környezetben is működőképes."[15]

„Ennek az egyet nem értésnek a terméke, hogy az elmúlt három évtized alatt, a világszervezeti statisztikákat jegyzők szerint 109 féle meghatározás, értelmezés született, de még mindig nem létezik mindenki számára elfogadható, egységes megközelítés."[16]

Mindezek ellenére a terrorizmus fogalma megjelenik a nemzetközi jog különböző forrásaiban. Globális szinten többek között általános és szektorális nemzetközi egyezményekben, a Biztonsági Tanács határozataiban, regionális szinten például az Európa Tanács és az Európai Unió által alkotott jogforrásokban. Az írott források mellett a jogtudomány képviselői által kialakított másik álláspont szerint a terrorizmus fogalma már létezik a nemzetközi szokásjogban is.[17] Ez az általam is leginkább támogatott megközelítés megjelent a bírói gyakorlatban is. A nemzetközi szokásjog alkalmazását a terrorizmus fogalmának meghatározásában részletesen elemezte a Libanoni Nemzetközi Törvényszék Fellebbviteli Kamarájának 2011. február 16-án hozott egyhangú döntése, amely a korábbi libanoni miniszterelnök Rafik Hariri ellen 2005. február 14-én végrehajtott merénylet elkövetőinek felelősségre vonásával foglalkozott.[18] Döntésében a bíróság kimondta, hogy a szokásjog alapján a terrorizmus fogalmának három eleme különböztethető meg: (1) bűncselekmény elkövetése vagy az ezzel való fenyegetés; (2) a szándék, hogy ez a cselekmény félelmet keltsen a lakosságban, vagy közvetlenül, vagy

[15] GYŰRŰ Attila: A terrorizmus fogalma a nemzetközi jogban 2015. június Themis, 113. http://epa.oszk.hu/02300/02363/00023/pdf/EPA02363_THEMIS_2015_jun_113-140.pdf

[16] GYŰRŰ Attila: i.m.120.

[17] A nemzetközi szokásjog a nemzetközi jog általánosan elfogadott forrása, ami jellemzően a nemzetközi jog elsődleges szereplőinek, az államoknak a gyakorlatban folytatott tevékenységéből kristályosodott ki. A szokásjog egyike a hágai Nemzetközi Bíróság Statútumában szereplő jogforrásoknak, a Statútum 38. cikkének definíciója szerint a „*jog gyanánt elismert általános gyakorlat bizonyítéka*". A jogtudomány képviselőinek döntő többsége a szokásjogi norma létét hagyományosan két konstitutív elem egyidejű létéhez köti: ez az állami gyakorlat (objektív vagy materiális elem), illetve az *opinio iuris*, vagyis az államok jogi meggyőződése arról, hogy gyakorlati tevékenységük a nemzetközi szokásjog szabályaival összhangban van (szubjektív vagy pszichológiai elem). Lásd: HOFFMANN Tamás: A nemzetközi szokásjog szerepe a magyar büntetőbíróságok joggyakorlatának tükrében http://jesz.ajk.elte.hu/hoffmann48.html és GYŰRŰ Attila: uo.131-132.

[18] http://www.stl-tsl.org/en/the-cases/stl-11-01/rule-176bis/filings/orders-and-decisions/appealschamber/f0010

közvetve arra kényszerítsen egy nemzeti vagy nemzetközi szervezetet, hogy valamely magatartást tanúsítson, vagy attól tartózkodjon; (3) a cselekmény foglalja magában a nemzetközi elemet.

Ebből a levezetésből is jól látszik, hogy a számos vita ellenére jogirodalmi szinten bizonyosan meghatározhatók azok keretek, amelyek a terrorizmus definiálásához szükségesek.

3. A privacy védelmének és korlátozásának modelljei a terrorizmus elleni fellépésben

A téma részletes elemzés előtt előre bocsátani, hogy tanulmányom további részében elsősorban a privacynek a személyes adatok védelméhez fűződő aspektusaira koncentrálok, ami persze nem jelenti azt, hogy az említett információs privacy mellett nem jelennek majd meg olyan példák, melyek a privacy egyéb aspektusaihoz sorolhatók. Ez annak is betudható, hogy a privacy egyes szeletei ilyen határozottan nem választhatók el egymástól.

Amint azt már a bevezetőben említettem, a privacy védelme és korlátozása a terrorizmus elleni fellépésben elsősorban nem abból a szempontból lényeges, hogy terrorcselekményt elkövetett személyek adataihoz a nyomozó hatóságok hogyan férhetnek hozzá. Ennél sokkal nagyobb társadalmi vitákat generál az emberek tömeges megfigyelése a mindennapi életük során, az őket érintő szivattyúszerű adatgyűjtés, és az adatok tárolása minden különösebb cél nélkül. Mindezt azzal az indokkal, hogy ezen adatok elemzése a nemzetbiztonság védelmének egyik hatékony eszköze.

A téma olyannyira ellentmondásos, hogy már a nyugati típusú demokráciák is megosztottak a kérdésben, az Európai Unió és az Egyesült Államok teljesen másképpen képzelik el a privacy védelmét és korlátozásának kereteit. Ennek részben történelmi, részben aktuálpolitikai indokai vannak.

4. A privacy védelmének modellje az Európai Unióban

Az Európai Unióban a természetes személyek személyes adatainak védelme alapvető jog. Az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Ez a jog azonban nem

csak az Európai Unión belül garantált, hanem az európai térségben is. Az emberi jogok és alapvető szabadságok védelméről szóló Egyezmény 8. Cikke szól a magán- és családi élet tiszteletben tartásához való jogról, mely kimondja, hogy „*mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák*." Előírja a jog korlátozásának szigorú szabályait is, kimondva, hogy „*e jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges*."

Mindkét említett alapjogi védelem erős bírósági kontrollal van körül bástyázva, amelyet az első esetben az Európai Unió Bírósága (a továbbiakban: EuB), a második esetben az Emberi Jogok Európai Bírósága (a továbbiakban: EJEB) biztosít.

Az említett alapjogvédelmi szabályok mellett az EU általánosságban védi a személyes adatokat és ezáltal a privacy ezen aspektusát, ami azt jelenti, hogy nem szektorális védelmet biztosítva különböztet az egyes ágazatok és annak védendő adatai között, hanem általános mércét határoz meg. Ezt egyrészt kiegészítik szektorális szabályok, másrészt az általános mérce szerint biztosított jogok is korlátozhatók, de csak szigorú feltételekkel.

a) Az Általános Adatvédelmi Rendelet és a Bűnügyi Adatvédelmi Irányelv

Az adatvédelem hatályos szabályait általánosságban az adatvédelmi irányelv[19] tartalmazza. Vannak természetesen szektorális szabályok, melyek közül kiemelendő a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló kerethatározat.[20] Annak ellenére, hogy ezek még hatályos szabályok, sokkal fontosabbak a manapság sokat emlegetett adatvédelmi reform termékei, melyek sok ponton alapjaiban változtatják meg az Európai Unió adatvédelmi politikáját. 2016. május 24-én hatályba lépett az általános adatvédelmi rendelet (a továbbiakban: GDPR),[21] amely

[19] Az Európai Parlament és a Tanács 95/46/ek irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

[20] A Tanács 2008/977/IB kerethatározata (2008. november 27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről

[21] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a

2 éves felkészülési időt követően 2018. május 25-től lesz alkalmazandó, hatályon kívül helyezve ezzel az adatvédelmi irányelvet. A GDPR, szemben az irányelvvel, közvetlenül alkalmazandó lesz valamennyi tagállamban. A kerethatározatot pedig irányelvi szabályozás fogja felváltani: a bűnügyi adatvédelmi irányelv[22] 2016. május 5-én lépett hatályba, és a tagállamoknak szintén 2 éves felkészülési időt követően, 2018. május 6-ig kell átültetniük azt a nemzeti jogrendjükbe. Mivel az adatvédelem irányát a jövőben az említett új jogszabályok fogják meghatározni, jelen írásban ezekre az új szabályokra leszek figyelemmel.

Az EU az adatvédelem területén általános, minden területre kiterjedő szabályzást kíván adni, és nem azon elv szerint védi a természetes személyek adatait, hogy azokat melyik ágazatban kezelik. Emellett természetesen megjelenik a szektorspecifikus védelem is, melynek jó példája a bűnügyi együttműködésről szóló irányelv, azonban ez nem érinti a védelem azon általános szintjét, melyet a GDPR kíván biztosítani.

A GDPR a tárgyi hatályáról a következőket mondja: *„E rendelet nem vonatkozik az alapvető jogok és szabadságok olyan tevékenységekkel kapcsolatos védelmére, illetve a személyes adatok olyan tevékenységekkel kapcsolatos szabad áramlására, amelyek az uniós jog hatályán kívül esnek, mint például a nemzetbiztonsággal kapcsolatos tevékenységek.”*[23] Főszabályként tehát a nemzetbiztonság védelmének keretében a privacyt korlátozó intézkedések a GDPR hatályának kívül maradnak. Ennek ellenére mégsem mondhatjuk azt, hogy ilyen esetekben az adatvédelmi követelményeket teljes egészében figyelmen kívül lehetne hagyni, melynek több oka is van. A GDPR 23. Cikke maga is említi a nemzetbiztonsági szempontokat, mint a jogok érvényesülésének korlátait. Ez azonban azt is jelenti, hogy bizonyos szempontból a nemzetbiztonsági célú adatkezelések is a GDPR hatálya alá tartoznak, csak az érintettek jogai korlátozásokkal érvényesülnek. Bizonyos korlátozásokkal tehát, de biztosított a védelemnek ez a szintje akkor is, ha a személyes adatok védelméhez fűződő jogot a nemzetbiztonsági szempontokkal kell összemérni. Nemzetbiztonsági érdekből sem mondható tehát, hogy az érintettek a GDPR által biztosított védelem nélkül maradnak. A jogok érvényesülésének már említett korlátai között szerepel a nemzetbiztonságnak egy esetleges terrorveszély által előidézett

95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

[22] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről

[23] GDPR (16) preambulum bekezdés és 2. Cikk (2) bekezdés a) pontja

potenciális sérelme. Ilyen esetekben is csak akkor alkalmazhatók bizonyos korlátozások, amennyiben azok tiszteletben tartják a jog lényeges tartalmát, és egy demokratikus társadalomban megfelelnek a szükségesség-arányosság mércéjének.[24] Általánosságban tehát azt mondhatjuk, hogy a privacy védelme és a nemzetbiztonsági érdekek összemérése esetén főszabályként a privacy védelme élvez elsőbbséget.

Mindezek alapján jól látható, hogy a GDPR által meghatározott adatkezelési alapelvek, mint a jogszerűség, a tisztességes eljárás és átláthatóság; a célhoz kötöttség; az adattakarékosság; a pontosság; a korlátozott tárolhatóság; az integritás és bizalmas jelleg; az elszámoltathatóság általános érvényesülést kívánnak és csak nagyon szigorú feltételekkel korlátozhatók. Ezen feltételeknek nem vagy csak nagyon szigorú keretek között felel meg a nemzetbiztonsági érdeken alapuló általános jellegű, konkrét cél nélküli adatgyűjtés és a prevenciós célú adatbányászat.

A GDPR számos más területen is szigorította az adatvédelmi szabályokat, ezzel is elismerve az információs privacy védelmének fontosságát az Európai Unióban. Jó példa erre a szankciók szigorítása. Az irányelv csak annyit mondott, hogy a *„tagállamok elfogadják a megfelelő intézkedéseket ezen irányelv rendelkezéseinek maradéktalan végrehajtása érdekében és különösen megállapítják az irányelv értelmében elfogadott rendelkezések megsértése esetén kiszabható szankciókat."* Ennek alapján minden tagállam viszonylag nagy mozgásszabadsággal rendelkezett a bírság mértékének meghatározásában. A GDPR ezzel szemben kimondja, hogy rendelkezéseinek megsértése miatt a jogsértő legfeljebb 10 000 000 EUR összegű közigazgatási bírsággal, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeggel sújtható, és a kettő közül a magasabb összeget kell kiszabni. Súlyos jogsértések esetén az összeg 20 000 000 EUR, illetve

[24] GDPR 23. Cikke szerint a rendeletben említett adatvédelmi alapelvek a rendeletben biztosított jogokkal összefüggésben korlátozhatók, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban: a) nemzetbiztonság; b) honvédelem; c) közbiztonság; d) bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését; e) az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot; f) a bírói függetlenség és a bírósági eljárások védelme; g) a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása; h) az a)–e) és a g) pontban említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység; i) az érintett védelme vagy mások jogainak és szabadságainak védelme; j) polgári jogi követelések érvényesítése.

vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeg.

Egy másik jó példa a GDPR szemléletváltására a rendelet extraterritoriális hatályának a koncepciója. Korábban jelentős vitákat generált az a kérdés, hogy a harmadik országbeli nagy szolgáltatók, különösen az USA-ban székhellyel rendelkező cégek, mint a Google, az Apple, a Microsoft, a Facebook a szolgáltatásaik nyújtása során mennyiben tartoznak az EU-s adatvédelmi szabályozás hatálya alá. Ez két szempontból is kulcsfontosságú kérdés: egyrészt ezek a cégek a személyes adatok hatalmas mennyiségét kezelik, másrészt az USA-ban hatályos *Patriot Act* szabályai alapján az USA igazságügyi szervei az Egyesült Államokban székhellyel, telephellyel rendelkező cégek esetében, de még azon cégek esetében is, amelyek tevékenysége az USA területére is irányul, hozzáférhetnek az általuk kezelt személyes adatokhoz.

A GDPR a hatályának meghatározása során hasonló logikát követ, kimondva, hogy a rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:

a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy

b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.

Azt, hogy ez a szabály, hogy fog működni a gyakorlatban, csak a joggyakorlat fogja megmutatni, azonban a jogalkotó a saját részéről a kérdést eldöntötte, a nagy harmadik országbeli szolgáltatók a GDPR hatálya alá tartoznak.

b) Az Emberi Jogok Európai Egyezménye és a Charta által biztosított védelem

Jelen tanulmány terjedelmét messze túllépné az említett nemzetközi jogi dokumentumokon alapuló bírósági esetjog bemutatása, ezért csak utalok arra, hogy a már említett két bíróság, nevezetesen az EuB és az EJEB, különösen a második, a témában kiterjedt esetjogot alakítottak ki, kimunkálva ezáltal azokat a feltételeket, amikor a privacy-t az egyes tagállamok jogalkotása és jogalkalmazása korlátozhatja.[25]

[25] Az EJEB privacy és terrorizmus témában kialakított esetjoga elérhető a Bíróság honlapján több tematikus

Terjedelmi korlátok miatt e munkában csak egy EJEB által eldöntött esetet mutatok be vázlatosan, tekintettel arra, hogy az ügy Magyarországot érinti. Ezt követően röviden megemlítek egy az EuB által eldöntött ügyet is, mely érintette az Alapjogi Charta által biztosított védelmet is.

A *Szabó és Vissy kontra Magyarország* ügyben a kérelmezők az Egyezmény 8. cikkére hivatkozva azt sérelmezték, hogy a *„7/E. § (3) bekezdése szerinti megfigyelés”* keretében akár indokolatlan és a magánéletet aránytalanul sértő intézkedéseknek is alanyai lehetnek, különösen bírósági kontroll hiányában.[26] A hatályos magyar jogszabályok a rendőrség feladatai közé sorolják a terrorizmus elleni fellépést. 2011. január 1-én a rendőrségen belül erre a célra megalakult a Terrorelhárítási Központ (TEK), amelynek hatáskörét a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: „Rtv.”) 7/E. §-a határozza meg. E jogszabály a titkos információgyűjtés során olyan különleges jogosítványokat biztosít a TEK számára, mint a titkos házkutatás és megfigyelés, ezek során felvétel készítése, postai küldemények felbontása, elektronikusan vagy számítógép útján továbbított kommunikáció megismerése és rögzítése – ráadásul ezekhez nem szükséges az érintett személyek hozzájárulása.

E tevékenységek engedélyeztetése a TEK által ténylegesen gyakorolt hatáskörtől függ, vagyis attól, hogy a tevékenységet olyan titkos megfigyelés keretében végzi-e, amely a törvény által felsorolt konkrét bűncselekmények felderítéséhez kapcsolódik (Rtv. 7/E. § (2) bekezdés), vagy a titkos információgyűjtés nemzetbiztonsági céllal valósul meg (7/E. § (3) bekezdés). Míg a Rtv. 7/E. § (2) bekezdése szerinti forgatókönyv ebben a formájában bírósági engedélyhez kötött, a 7/E. § (3) bekezdése szerinti tevékenységet már az igazságügyért felelős miniszter engedélyezi: (i) terrorcselekmények megakadályozása vagy Magyarország nemzetbiztonsági érdekeinek érvényesítése, illetve (ii) külföldi fegyveres konfliktus vagy terrorcselekmény esetén magyar állampolgárok mentése érdekében.

Az „Rtv. *7/E. § (3) bekezdése szerinti megfigyelés*” a nemzetbiztonsági szolgálatokról szóló törvény rendelkezései szerint történik, azzal a

---

dossziéban, melyek a következők: Terrorism http://www.echr.coe.int/Documents/FS_Terrorism_ENG.pdf ; Mass surveillance http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf és Protection of Personal Data http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

[26] Az ítélet angol nyelven a bíróság hivatalos honlapján: http://hudoc.echr.coe.int/eng#{"itemid":["001-160020"]};

magyarul az Eötvös Károly Közpolitikai Intézet honlapján: http://ekint.org/lib/documents/1480415991-Szabo_es_Vissy_itelet.pdf (2017.05. 06.)

megkötéssel, hogy csak akkor alkalmazható, ha a szükséges információ más módon nem szerezhető be. Egyébiránt a törvény semmilyen konkrét szabályt nem tartalmaz arra vonatkozóan, hogy milyen körülmények között rendelhető el az intézkedés, szemben az „Rtv. *7/E. § (2) bekezdése szerinti megfigyelés*" esetével, amely csak bizonyos súlyos bűncselekmények gyanújával végezhető. Az „Rtv. *7/E. § (3) bekezdése szerinti megfigyelés*" legfeljebb 90 napig végezhető, de ezt az időszakot a miniszter további 90 nappal meghosszabbíthatja. A miniszter ugyanakkor nem jogosult megismerni a folyamatban lévő megfigyelés eredményét, amikor döntenie kell a hosszabbításról. A megfigyelés befejezését követően a törvény semmilyen formában nem kötelezi a hatóságokat, hogy a megszerzett lényegtelen információkat megsemmisítsék.

A kérelmezők először a magyar Alkotmánybírósághoz fordultak. 2012. június 15-én alkotmányjogi panasszal éltek, amelyben lényegében azt állították, hogy az Rtv. 7/E. § (3) bekezdése által biztosított széles körű jogosítványok sértik a magánélet védelméhez fűződő alkotmányos jogaikat. Hangsúlyozták, hogy a jogszabály a nemzetbiztonsági célú titkos megfigyelés esetében kevesebb jogi garanciát határoz meg a magánélethez való jog védelmére, mint az egyes bűncselekmények felderítéséhez kapcsolódó titkos megfigyelés esetében.

2013. november 18-án hozott döntésében az Alkotmánybíróság a kérelmezők által megfogalmazott panaszok többségét elutasította. Az Alkotmánybíróság egy tekintetben igazat adott a kérelmezőknek: megállapította, hogy a titkos információgyűjtést elrendelő miniszternek indoklással kell alátámasztania a döntését. Lényegében azonban az Alkotmánybíróság úgy ítélte meg, hogy a nemzetbiztonsági feladatok köre jóval szélesebb, mint az egyes bűncselekmények felderítéséhez kapcsolódó feladatok köre. Szerintük nemzetbiztonsági ügyekben a valóság történéseit nem azok büntetőjogi relevanciája szempontjából vizsgálják, így azoknak nem is kell feltétlenül valamilyen bűncselekményhez kapcsolódniuk. Továbbá a nemzetbiztonsággal összefüggésben a miniszter által engedélyezett valamennyi megfigyelés külső ellenőrzését az Országgyűlés Nemzetbiztonsági Bizottsága látja el, amely a minisztertől általánosan és a konkrét ügyekre vonatkozóan is beszámolót kérhet. A külső ellenőrzésben részt vesz az ombudsman is. Ez a rendszer – az AB szerint – megfelelő garancia az érintettek magánélethez való alkotmányos jogának tiszteletben tartására. Végül az Alkotmánybíróság véleménye szerint a nemzetbiztonsági szolgálatokról szóló törvény, amely a Rtv. 7/E. § (3) bekezdése szerinti megfigyelésről is rendelkezik, tartalmaz általános rendelkezéseket arra vonatkozóan, hogy

az információgyűjtéssel elérni kívánt cél szempontjából felesleges adatokat hivatalból törölni kell.

A kérelmezők ezt követően 2014. május 13-án fordultak a strasbourgi bírsághoz. Az EJEB a kérelmet befogadhatónak minősítette, és kimondta a kérelmezők áldozati státuszát,[27] és a hazai jogorvoslatok kimerítését.[28] A Bíróság az érdemi vizsgálat keretében megvizsgálta az Egyezmény 8. Cikk 2. pontjában foglalt feltételek érvényesülését. Álláspontja szerint a törvényben meghatározottság követelménye teljesült, mert a kérdéses beavatkozás célja a nemzetbiztonság védelme és/vagy zavargás vagy bűncselekmény megelőzése. Másfelől viszont meg kell bizonyosodni arról, hogy az említett cél megvalósításához a kifogásolt jogszabályban rögzített eszközök minden tekintetben annak a keretei között maradnak-e, ami egy demokratikus társadalomban szükséges.[29]

A Bíróság szerint, amikor meg kell határozni az egyensúlyt az alperes állam azon érdeke, hogy nemzetbiztonságát titkos megfigyelés révén védelmezze, valamint a kérelmezők magánélethez való jogába történő beavatkozás súlyossága között, az állami hatóságoknak van bizonyos mértékű mérlegelési joga annak megválasztásában, hogy a nemzetbiztonság megvédésének jogos célját milyen eszközökkel érjék el. Ez a mérlegelési jogkör azonban európai szintű felülvizsgálat alá esik mind a jogszabályok, mind a jogalkalmazói döntések terén. Figyelemmel arra, hogy a nemzetbiztonság védelme érdekében felállított titkos megfigyelési rendszer a demokrácia oltalmazásának leple alatt alááshatja vagy akár le is rombolhatja azt, a Bíróságot meg kell győzni arról, hogy megfelelő és hatékony garanciák állnak rendelkezésre a visszaélések

[27] A Bíróság elfogadta, hogy bizonyos körülmények között az egyén áldozatnak tekintheti magát pusztán a titkos megfigyelést lehetővé tévő jogszabály létezése miatt is, jóllehet ilyen konkrét intézkedés őt magát nem érintette (az ítélet 33. pontja). A Bíróság észrevételezte, hogy a civil szervezethez kötődés nem szerepel a jogszabályban felsorolt jogalapok között, ahol lényegében csak a terrorcselekmény veszélyével és a magyar állampolgárok külföldi mentésével kapcsolatos jogalapok szerepelnek. Ugyanakkor úgy tűnik, hogy e rendelkezések szerint bármely Magyarországon tartózkodó személy kommunikációját megfigyelhetik, ha a megfigyelést a törvényben felsorolt jogalapok alapján szükségesnek ítélik meg (az ítélet 16. bekezdése). A Bíróság szerint nem zárható ki annak a lehetősége, hogy a kérelmezőkkel szemben ilyen intézkedéseket alkalmaznak, ha a hatóságok megítélése szerint ez a jogszabályban foglalt veszélyek megelőzéséhez vagy megakadályozásához célszerű, különösen, ha figyelembe vesszük a törvény szóhasználatát („az érintett vagy érintettek … köre"), amely valóban bárkit magában foglalhat (az ítélet 38. pontja).

[28] A hazai jogorvoslati lehetőségek kimerítését illetően a Bíróság kielégítőnek találja azt, hogy a kérelmezők a nemzeti hatóságok – jelen esetben az Alkotmánybíróság – tudomására hozták sérelmük érdemi részét, vagyis azt, hogy az Rtv. 7/E. § (3) bekezdése szerinti megfigyelésre vonatkozó szabályok nem biztosítanak elegendő garanciát (az ítélet 40. pontja).

[29] A titkos megfigyelési intézkedésekre vonatkozó esetjogában a Bíróság a következő minimális garanciákat dolgozta ki, amelyeket a hatalommal való visszaélés megelőzésére a törvénybe be kell építeni: a beavatkozást elrendelő végzés alapjául szolgáló bűncselekmények jellege; a telefonbeszélgetések lehallgatásával érintett személyek kategóriáinak meghatározása; a lehallgatás időtartamára vonatkozó korlát; a megszerzett adatok vizsgálatára, felhasználására és tárolására vonatkozó eljárás; az adatok másokkal való közlése esetén alkalmazandó óvintézkedések; valamint milyen körülmények között kell a rögzített adatokat törölni vagy megsemmisíteni (az ítélet 56. pontja).

megelőzésére. A vizsgálat függ az ügy valamennyi körülményétől, így a lehetséges intézkedés jellegétől, körétől és időtartamától, az elrendelésükhöz szükséges jogalaptól, az engedélyező, végrehajtó és felügyelő hatóságok körétől, valamint a nemzeti jog által biztosított jogorvoslat fajtájától. A Bíróságnak meg kell állapítania, hogy a korlátozó intézkedések elrendelését és végrehajtását felügyelő eljárások képesek-e biztosítani, hogy a „*beavatkozás*" olyan legyen, ami egy „*demokratikus társadalomban szükséges*". A kérelmezőknek arról a kifogásáról, mely a jogszabályi rendelkezések nem kellően világos és nem kellően előreláthatóvoltát bírálta, kimondták: a Bíróság számára a jogszabály „előreláthatóságának" követelménye nem értelmezhető olyan tágan, hogy az államok kötelesek lennének a jogszabályban a titkos megfigyelés megindításához szükséges döntést kiváltó valamennyi helyzetet részletesen felsorolni. A terrorizmus veszélyére vagy mentési műveletre való hivatkozás elvben úgy tekinthető, hogy feltüntették az állampolgárok számára az okokat. Súlyos aggodalomra ad okot ugyanakkor, hogy az „érintett vagy érintettek … köre" fogalmába valóban bárki beletartozhat, így az állampolgárok tömeges és korlátlan megfigyeléséhez vezető út kikövezéseként is értelmezhető. A Bíróság megjegyzi, hogy nincs a hazai jogban világos rendelkezés arról, hogyan kell ezt a fogalmat a gyakorlatban alkalmazni.

A Bíróság szerint napjaink terrorcselekményeinek megnyilvánulási formáiból természetesen következik az, hogy a kormányok a legmodernebb technológiák segítségével igyekeznek megakadályozni az ilyen támadásokat, ideértve azoknak a kommunikációknak a tömeges felügyeletét is, amelyek utalhatnak a közelgő incidensekre. E felügyeleti tevékenységhez használt technikák az elmúlt években figyelemreméltó fejlődésen mentek keresztül, és olyan kifinomulttá váltak, melyet egy átlagos állampolgár már nehezen fog fel. Különösen, azért, mert már az automatikus és rendszerszerű adatgyűjtés is technikailag lehetővé, sőt széles körben alkalmazottá vált. Ennek fényében a Bíróság köteles megvizsgálni, hogy a tömeges adatgyűjtést eredményező megfigyelési módszerek fejlődésével együtt fejlődtek-e az állampolgárok Egyezményben foglalt jogait biztosító garanciák is. A magánélethez való jogra leselkedő ilyen fokú veszélyt nagyon szoros felügyelet alatt kell tartani mind nemzeti szinten, mind pedig az Egyezmény értelmében. Az Egyezményhez kapcsolódó esetjogban a megfigyelésekkel szemben megkövetelt garanciákat úgy kell továbbfejleszteni, hogy azok kezeljék az ilyen megfigyelési gyakorlatok kérdését is. A vizsgálat ügyben azonban a Bíróságnak nem kellett kitérnie erre a kérdésre, mivel a magyar

garanciarendszer láthatóan még a korábban megfogalmazott alapelveknek sem tesz eleget.

Ugyanakkor a kérdéses beavatkozás sajátos jellegét és az állampolgárok magánszférájának megsértésére alkalmas megfigyelési csúcstechnológiát figyelembe véve, a Bíróság szerint az „egy demokratikus társadalomban szükséges két követelményt ebben az összefüggésben két szempontból is „szigorúan szükséges”-ként kell értelmezni. Egy titkos megfigyelési intézkedés csak akkor lehet összhangban az Egyezménnyel, ha az – általános megfontolásként – szigorúan szükséges a demokratikus intézmények védelméhez, valamint – konkrét megfontolásként – szigorúan szükséges a kulcsfontosságú információk megszerzéséhez egy adott műveletben. A Bíróság szerint minden olyan titkos megfigyelési intézkedés, amely nem felel meg ezeknek a követelményeknek, lehetőséget kínál a félelmetes technológiákhoz hozzáférő hatóságoknak a visszaélésére. A Bíróság álláspontja szerint a törvény szövegezéséből – különösen bírósági értelmezés hiányában – nem derül ki világosan, hogy a megfigyelésre adott engedélyt csak egyszer vagy akár többször is meg lehet hosszabbítani, ami újabb visszaélésekre adhat lehetőséget.

A megfigyelés jóváhagyása szintén aggályokat vet fel. Az intézkedést az igazságügyért felelős miniszter engedélyezi az illetékes nemzetbiztonsági szolgálatok, vagyis a TEK vezetőinek javaslatára. Ez a szervezet a rendőrségen belül taktikai feladatokat lát el, szervezetileg a Belügyminisztérium alá tartozik, és a terrorellenes küzdelemben kiterjedt különleges jogosítványokkal rendelkezik arra, hogy kényszert alkalmazzon. A Bíróság szerint ez a felügyelet – amely priméren politikai jellegű, bár a TEK-től és a Belügyminisztériumtól formálisan független igazságügyi miniszter látja el – lényegénél fogva nem képes biztosítani, hogy a visszaélésnek kitett célok és eszközök szempontjából értékeljék a szigorú szükségesség követelményét.

Ami a megfigyelés engedélyezésére illetékes hatóságot illeti, nem feltétlenül sérti az Egyezményt, ha nem bíróság engedélyezi a telefonlehallgatást, de a Bíróság szerint ebben az esetben a hatóságnak kellően függetlennek kell lennie a végrehajtó hatalomtól. Az engedélyezés és felügyelet politikai jellege miatt azonban nagyobb a kockázata annak, hogy az intézkedésekkel visszaéljenek. A Bíróság szerint a végrehajtó hatalom politikai felelősséget viselő tagja – így pl. az igazságügyi miniszter – nem nyújt megfelelő garanciát.

A jogszabály ezen kívül rendkívül sürgős esetekben azt is lehetővé teszi, hogy a nemzetbiztonsági szolgálatok főigazgatói a titkos

információgyűjtés folytatását legfeljebb 72 órára engedélyezzék. A Bíróság szerint ez a különleges jogkör elegendő minden olyan esetre, amikor a külső, bírósági ellenőrzés alkalmazásával a hatóságok értékes időt veszítenének el. Ezeket az intézkedéseket azonban utólagos felülvizsgálathoz kell kötni, ami főszabály szerint mindig szükséges, ha a megfigyelést előzetesen nem bírósági szerv engedélyezte. A Bíróság azonban nem talált olyan rendelkezést a magyar jogszabályokban, amely a titkos megfigyelés alkalmazása során jogorvoslatot biztosítana azok számára, akiket a titkos megfigyelés érintett, de erről – mivel azt a szükség úgy kívánta – nem értesültek. Az érintettek számára biztosított jogorvoslati lehetőségekről a Bíróság kimondta, hogy a nemzetbiztonsági törvényben rögzített panasztételi eljárás csekély jelentőségű, hiszen a titkos megfigyeléssel érintett állampolgárok nem értesülnek a velük szemben alkalmazott intézkedésekről.

A Bíróság említést tett továbbá a kérelmezők által benyújtott bizonyítékról, amely szerint az alapvető jogok biztosa eddig még egyszer sem vizsgált titkos megfigyeléssel kapcsolatos ügyet. A Bíróság felidézte, hogy a *Klass és társai ügyben* elfogadhatónak találta azt az egyesített felügyeleti mechanizmust, amelyben nem volt formális bírósági kontroll, de *„az ellenőrzés első körét bírói hivatal betöltésére képesítéssel rendelkező tisztviselő végezte*”. A magyar engedélyezési folyamatban azonban nem vesz részt ilyen tisztviselő. A felek nem bizonyították, hogy a magyar alapvető jogok biztosa szükségszerűen bírói tisztséget is betölt vagy betöltött.

A Bíróság ezen kívül megállapította, hogy a titkos megfigyelésről való utólagos értesítés elválaszthatatlanul kapcsolódik a megfigyelési jogokkal való visszaéléssel szembeni jogorvoslatok hatékonyságához, és így a hatékony garanciák meglétéhez is. Másképp az érintett egyénnek nem sok lehetősége van a jogorvoslatra, hacsak nem értesítik a vele szemben, de tudta nélkül tett intézkedésekről, és így biztosítják, hogy utólagosan vitassa azok indokoltságát. Amint az értesítés a megfigyelést követően a korlátozás céljának veszélyeztetése nélkül kiküldhető, azt meg is kell küldeni az érintetteknek. A magyar jog szerint azonban az intézkedésekről semmilyen értesítést nem kell küldeni. Ez a tény a visszaélésekkel szemben elérhető formális jogorvoslat hiányával együtt azt mutatja, hogy a jogi szabályozásból hiányoznak a megfelelő garanciák.

Összességében a Bíróságnak kétségei maradtak afelől, hogy az Rtv. 7/E. § (3) bekezdése szerinti megfigyelést szabályozó magyar jogszabály megfelelően pontos, hatékony és átfogó jogi garanciákat biztosítana a

megfigyelő intézkedések elrendelésével, végrehajtásával és a vonatkozó jogorvoslati lehetőségekkel kapcsolatban. Mivel az intézkedések köre gyakorlatilag bárkire kiterjedhet, és az intézkedések elrendelése teljes egészében a végrehajtó hatalom hatáskörében történik, mégpedig a szigorú szükségesség elvének mérlegelése nélkül, továbbá a legújabb technológiák révén a Kormány akár az intézkedés eredeti hatályán kívül eső személyekről is könnyedén és tömegesen szerezhet adatokat, valamint nemhogy bírósági, de semmilyen egyéb hatékony jogorvoslati lehetőség nem biztosított, a Bíróság arra a következtetésre jutott, hogy megsértették az Egyezmény 8. cikkét.

Amint azt a jelen fejezet elején említettem, az EJEB mellett az EuB is foglalkozik a privacy és terrorizmus összefüggéseit érintő ügyekkel. Jó példa erre az adatmegőrzési irányelv[30] megsemmisítése. Az adatmegőrzési irányelv a nyilvános hírközlő hálózatokon kizárólag a forgalmi adatok (kommunikáció tartalmára vonatkozó adatok nélküli) megőrzését tette kötelezővé közbiztonsági okokból 6 hónap és két év közötti időtartamban az elektronikus hírközlési szolgáltatások nyújtói, illetve a nyilvános hírközlő hálózatok szolgáltatói számára, tehát súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából. A Bíróság álláspontja szerint az irányelv anélkül teszi lehetővé az adatokhoz való hozzáférést, hogy megfelelő garanciákat tartalmazna a hozzáférés szükséges és arányos adatokra való korlátozására.[31]

c) A tagállami bíróságok által biztosított védelem

Tekintettel arra, hogy az EU-ban nincs és a tagállami szuverenitás e területen való kiemelt jelentősége miatt talán nem is lehet egységes szabályozás a nemzetbiztonság területén, számos ügyet tárgyalnak a nemzeti bíróságok, melyek adott esetben el sem jutnak az EU vagy az Európa Tanács valamely fórumára. A tagállami bírósági döntések közül még a legfontosabbak említése is messze túllépné jelen tanulmány kereteit, ezért csak egyetlen esetet említek, mely jól érzékelteti a kérdés jelentőségét és egyben a tagállami és EU-s hatáskörök közötti konfliktust.

A német szövetségi Alkotmánybíróság 2013. április 24-én hozott döntést a központi antiterrorizmus adatbázis szabályozását (Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und

[30] http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=526042

[31] Liber Ádám: Érvénytelen az adatmegőrzési irányelv. http://www.dataprivacy.hu/?p=1295 (közzétéve: 2014/04/10.; a letöltés időpontja: 2017. május 6.)

Nachrichtendiensten des Bundes und der Länder; benannt als Gemeinsame-Dateien-Gesetz) érintő ügyben.[32] A törvény alapján lehetőség van a rendőrség és a nemzetbiztonsági szervek által használt adatbázisok összekapcsolására tartományi és szövetségi szinten, és a hatóságok közötti információcserére, mely hatékonyabb együttműködést biztosít az egyes hatóságok között a terrorizmus ellen fellépés területén is. A kérelmező szerint a rendelkezések sértik az érintettek magánszférájához fűződő jogot, mivel érdemi korlátozások nélkül biztosítanak lehetőséget személyes adatok tárolására és cseréjére.

A német Alkotmánybíróság az ügyben a következőket mondta ki:

● Alapjában véve összeegyeztethető az alkotmánnyal, hogy olyan anti-terrorizmus adat(bázis) kerüljön létrehozásra, mely a különböző, szövetségi szintű biztonsági szervezetek rendelkezésére álló adat(bázis)okat kötné össze és a nemzetközi terrorizmus leküzdése érdekében folytatott munkavégzéséhez járul hozzá, feltéve, hogy ennek az adat(bázis)nak az elsődleges célja az információátadás az egyes szervek között és az információ/adat felhasználása csak kivételes(en sürgős) esetekben, a szervek operatív tevékenysége ellátása érdekében történik.

● Az olyan (jog)szabályok, melyek lehetővé teszik a rendőri és nemzetbiztonsági szervek közötti adatátadást/szolgáltatást, az információs szabadság mint alapjog követelményeinek való megfelelés szempontjából szigorúbb alkotmányjogi vizsgálat alá esnek (szigorúbb alkotmányjogi követelményeknek kell megfelelniük). Az alapjogok természetéből fakadóan az adatokat egymástól elkülönítve kell kezelni. Az adatösszekapcsolás tilalma az információátadást csak kivételes esetekben teszi lehetővé.

● Olyan szövetségi szintű, a biztonsági szervek adatbázisait összekötő adatbázis, mint az antiterrorizmus adatbázis létrehozása csak a joggal való visszaélés lehetőségét kizáró törvényi szabályozással történhet, mely messzemenőkig pontosan felsorolja a kezelt adatok körét és azok felhasználásának módját/felhasználási lehetőségeit. Az antiterrorizmus adatbázis e követelménynek nem felel meg teljesen, mégpedig a következő tárgykörökben: a részt vevő hivatalok (közjogi szervezetek) meghatározása; a „terrorizmusközeli”-nek tekintett személyek köre; a kontaktszemélyek bevonása; a titokban rendelkezésre bocsátott,

[32] http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2013/04/rs20130424_1bvr121507.html Letöltés időpontja: 2017.05.06.

kibővített/szélesebb körű alapadatok felhasználása; a biztonsági szervezetek rendelkezésére álló, tárolható adatok köre és ennek hatékony felügyelete.

● Az olyan adatok korlátlan felvétele az antiterrorizmus adatbázisba, melyeket a levél- és távirati titok, ill. a magánlak sérthetetlenséghez fűződő jog megsértésével gyűjtenek össze, a Grundgesetz (GG) 10. cikk (1) bekezdésébe és a 13. cikk (1) bekezdésébe ütközik.

Ez az ítélet nemcsak a tartalma miatt érdekes. 2013 februárjában az EuB döntést hozott a *Fransson ügyben*, mely ismét megnyitotta a vitát arról, hogy az Alapjogi Charta 51. cikk (1) bekezdése alapján mikor van lehetőség a nemzeti jog alapjogi vizsgálatát kérni EuB-től a Chartával való ellentétre hivatkozással.[33] A német Alkotmánybíróság elutasítva azt a lehetőséget, hogy az EuB a döntését vizsgálja, részletesen elemzi, hogy a jogszabály a nemzeti jog hatálya alá tartozó célokat érvényesít, és azt, hogy az EU az adatvédelem és a terrorizmus elleni fellépés területén is alkotott jogszabályokat, valamint azt, hogy a nemzeti jogszabály által szabályozott igazságügyi együttműködés, az EU által e területen alkotott szabályok érvényesülését befolyásolhatja. Mindezek ellenére a német Alkotmánybíróság véleménye szerint a német szabályozás csak részben és közvetetten kapcsolódik az említett területeken alkotott jogszabályi célokhoz. Ezáltal a németek maguk mondták ki, hogy az ügyben a Alapjogi Charta nem alkalmazható, mivel az EU jog nem írja elő antiterrorizmus adatbázis létrehozását, de azt nem is tiltja meg és nem szabályozza annak jellemzőit.

Felhasznált irodalom

Alan WESTIN (1967): Privacy and Freedom. Atheneum, New York

David LYON: Surveillance after September 11. Polity Press, Cambridge 2003.

GYŰRŰ Attila: A terrorizmus fogalma a nemzetközi jogban. Themis, 113. 2015. június

[33] Az Alapjogi Charta 51. cikk (1) bekezdése az alkalmazási kör keretében kimondja, hogy „e Charta rendelkezéseinek címzettjei – a szubszidiaritás elvének megfelelő figyelembevétele mellett – az Unió intézményei, szervei és hivatalai, valamint a tagállamok annyiban, amennyiben az Unió jogát hajtják végre. Ennek megfelelően saját hatáskörükben és a Szerződésekben az Unióra ruházott hatáskörök korlátain belül tiszteletben tartják az ebben a Chartában foglalt jogokat és betartják az abban foglalt elveket, valamint előmozdítják azok alkalmazását." Az 51. cikk (2) bekezdése azonban azt is kimondja, hogy „ez a Charta az uniós jog alkalmazási körét nem terjeszti ki az Unió hatáskörein túl, továbbá nem hoz létre új hatásköröket vagy feladatokat az Unió számára, és nem módosítja a Szerződésekben meghatározott hatásköröket és feladatokat."

Patrick Troy HATFIELD: The Great Divide: Recent Trends Could Help Bridge the US/EU Data Privacy Gap 4-24-2016 Seattle Journal for Social Justice Volume 14, Issue 1.

Rachel L. FINN, David WRIGHT and Michael FRIEDEWALD: Seven Types of Privacy 2013. Frauenhofer Institue for Systems and Innovation Research

Roger CLARK: Introduction to datavaillance and Information Privacy, and Definitions of Terms, Xamax Consultancy, Aug1997. http://www.rogerclarke.com/DV/Intro.html

Sissela BOK (1983): Secrets On the Ethics of Concealment and Revelation. New York: Pantheon Books

SZABÓ Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. Információs Társadalom, 2005. 2. szám. 44-54.

WARREN and BRANDEIS: The Rights to Privacy. Harward Law review Vol. IV. December 15, 1890 No. 5

***

Privacy and Terrorism

Summary

Is it possible to maintain privacy while living under the threat of terrorism? How far can government agencies go to protect their citizens? These are the questions that are all too frequently being asked in the light of the events of 11 September 2001 and the continuing threat of terrorism since then, where a fresh incident is reported almost every month. The war on terror has stepped up to a considerably new level as far as national security is concerned and governments throughout the world are using the cutting edge of technology to track down terrorists but at the expense of our privacy. In the first part of my new article I attempt to introduce this current and compelling topic first by giving an interpretation of the two terms, privacy and terrorism, and after giving an insight into the privacy regime of the European Union.